WEEKLY THREAT BRIEF // ALL COLLECTED

Bottom line

We reviewed 107 threat campaigns this week, of which 106 rated High or Critical. Pressure concentrated on Technology and adjacent sectors. The most repeated attacker objective points to a clear, single defensive priority described below.

Threat landscape

The most active named actors were The Gentlemen, APT37, Gamaredon, DragonForce. Targeting clustered around United States of America, India, Taiwan, Ukraine, with Technology, Government, Finance, Education absorbing the most activity.

Where to focus

Across the week, attackers most often converged on the same objective (Registry Run Keys / Startup Folder), which was the decisive control point in 19 separate campaigns. Prioritising the controls that break that step is the single highest-leverage move for the coming week.

Notable campaigns

- Critical: Interlock and Rhysida within the Ransomware Ecosystem (linked to Hive0163)
- Critical: Hacktivists are broadening their scope beyond political motivation (linked to 4BID)
- Critical: Old WinRAR Flaw Fuels Attacks on Ukraine: How Unmanaged Software Keeps the Door Open (linked to Earth Dahu)
- Critical: From emerging threat to top-tier ransomware-as-a-service: The evolution of INC ransomware (linked to INC)

Outlook

These figures describe what we collected this week and should be read as a snapshot, not a forecast. We will track whether the dominant technique persists as more weeks accumulate.

Appendix // The week by the numbers

Derived from 107 unique campaigns collected this period. Every figure below is a direct count, not an estimate.

Severity

Band	Campaigns
Critical	79
High	27
Moderate	1

Sectors targeted

Sector	Campaigns
Technology	25
Government	25
Finance	17
Education	12
Healthcare	11
Defense	9

Geographies

Country	Campaigns
United States of America	15
India	9
Taiwan	6
Ukraine	6
Canada	6
Brazil	5

Most active actors

Actor	Campaigns
The Gentlemen	5
APT37	3
Gamaredon	3
DragonForce	2
SilverFox	2
GOLD PRELUDE	2

Malware families

Family	Campaigns
Vidar	11
Cobalt Strike	10
ValleyRAT	6
Sliver	5
Mimikatz	4
Remcos RAT	4
SocGholish	3
SystemBC	3

CVEs in play

CVE	Campaigns
CVE-2025-8088	4
CVE-2025-5777	2
CVE-2024-55591	2
CVE-2026-50751	1
CVE-2026-50752	1
CVE-2023-52271	1

Defensive priority // recurring chokepoints

The techniques that were the decisive control point in the most campaigns. Hardening these is the highest-leverage move for the period.

Technique	Control point	Campaigns
T1547.001	Registry Run Keys / Startup Folder	19
T1112	Modify Registry	18
T1078	Valid Accounts	9
T1566	Phishing	9
T1190	Exploit Public-Facing Application	5
T1195.002	Compromise Software Supply Chain	5

What we observed this week, by sector

Most common chokepoint per sector this week; the count is out of that sector's campaigns. A description of what we saw, not a coverage guarantee.

Sector	Technique	Control point	Seen
Technology	T1547.001	Registry Run Keys / Startup Folder	4/25
Government	T1547.001	Registry Run Keys / Startup Folder	10/25
Finance	T1547.001	Registry Run Keys / Startup Folder	5/17
Education	T1566	Phishing	3/12
Healthcare	T1547.001	Registry Run Keys / Startup Folder	4/11
Defense	T1112	Modify Registry	4/9

Notable campaigns (expanded roster)

Severity	Campaign	Attributed to
Critical	Interlock and Rhysida within the Ransomware Ecosystem	Hive0163
Critical	Hacktivists are broadening their scope beyond political motivati	4BID
Critical	Old WinRAR Flaw Fuels Attacks on Ukraine: How Unmanaged Software	Earth Dahu
Critical	From emerging threat to top-tier ransomware-as-a-service: The ev	INC

Severity	Campaign	Attributed to
Critical	Attackers Weaponize Microsoft Teams Relays to Stay Hidden	DragonForce
Critical	Ongoing exploitation of Cisco Catalyst SD-WAN vulnerabilities	UAT-8616
Critical	Vidar Stealer Unmasked: Code Signing Abuse, Go Loaders and File	X3D MINER
Critical	LBIOC-20260071 - The Gentlemens Leak	The Gentlemen
Critical	Targets Education Sector with Oracle PeopleSoft Exploit	UNC6240
Critical	The Gentlemen are knocking: custom backdoors and evolving tactic	The Gentlemen